Advisory 2019-08

CODESYS V3 various products password transmission vulnerability

Published: 18 December 2019

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2019-08_CDS-62813.docx

CONTENT

		Page
1	**Affected Products**	**3**
2	**Vulnerability overview**	**3**
2.1	Type	3
2.2	Management Summary	3
2.3	References	3
2.4	Severity Rating	3
3	**Vulnerability details**	**3**
3.1	Detailed Description	3
3.2	Exploitability	3
3.3	Difficulty	3
3.4	Existence of exploit	4
4	**Available software updates**	**4**
5	**Mitigation**	**4**
6	**Acknowledgments**	**4**
7	**Further Information**	**4**
8	**Disclaimer**	**5**
Bibliography		**6**
Change History		**6**

1 Affected Products

All variants of the following CODESYS V3 products in all versions containing the CmpUserMgr component are affected, regardless of the CPU type or operating system:
• CODESYS Control for BeagleBone
• CODESYS Control for emPC-A/iMX6
• CODESYS Control for IOT2000
• CODESYS Control for Linux
• CODESYS Control for PFC100
• CODESYS Control for PFC200
• CODESYS Control for Raspberry Pi
• CODESYS Control RTE V3
• CODESYS Control RTE V3 (for Beckhoff CX)
• CODESYS Control Win V3 (also part of the CODESYS Development System setup)
• CODESYS V3 Simulation Runtime (part of the CODESYS Development System)
• CODESYS Control V3 Runtime System Toolkit
• CODESYS HMI V3

2 Vulnerability overview

2.1 Type

Insufficiently protected transport of credentials

2.2 Management Summary

Without using the TLS based encrypted CODESYS online communication, the user credentials are insufficiently protected on transport.

2.3 References

CVE: CVE-2019-9013 [6]

ICS-CERT: ICSA-19-213-04 [8]

CODESYS JIRA: CDS-62813

2.4 Severity Rating

3S-Smart Software Solutions GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 8.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. The CODESYS Control runtime system provides several security features. To limit the access to the programming port, it allows defining users with individual passwords or also to configure a role based user management with graded access rights and multiple users. Without using the TLS based encrypted CODESYS online communication, the user credentials are insufficiently protected on transport.

3.2 Exploitability

To exploit this vulnerability, an attacker needs access to the online communication traffic to the PLC.

3.3 Difficulty

An attacker with low skills would be able to exploit a PLC without activated communication encryption.

3.4 Existence of exploit

No known public exploits specifically target this vulnerability, but we do know some publicly available information that would allow an exploit to occur.

4 Available software updates

This issue will be fixed by version V3.5.16.0 of the affected products.
The release of version V3.5.16.0 is expected for May 2020.

5 Mitigation

As long as no bug fix is available, 3S-Smart Software Solutions GmbH strongly recommends activating and using encryption of online communication whenever possible. The encrypted communication protects the password transmission by a TLS based encryption, independent of the weak password encryption affected here.

The encryption of the online communication and the online user management of CODESYS control runtime systems is already available since several service packs of the affected products. Depending on the PLC runtime system, these features can be activated by the user or only by the control manufacturer. Further information on how to activate encrypted communication and user management can be found in the CODESYS online help.

3S-Smart Software Solutions GmbH recommends as part of the mitigation strategy the following defensive measures to reduce the risk of exploitation of this vulnerability:
• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
• Use firewalls to protect and separate the control system network from other networks
• Use VPN (Virtual Private Networks) tunnels if remote access is required
• Activate and apply user management and password features
• Limit the access to both development and control system by physical means, operating system features, etc.
• Protect both development and control system by using up to date virus detecting solutions
For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [1].

6 Acknowledgments

3S-Smart Software Solutions GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

We thank the following researchers for reporting this vulnerability independently from each other following coordinated disclosure:
• Nico Jansen from FH Aachen University of Applied Sciences
• Kaspersky Lab ICS CERT
• Martin Hartmann from cirosec GmbH
• Lab. of Information Systems Security Assurance (Kangbin Yim, Eunseon Jeong, Junyoung Park, Jeonghyeon Gim, Byeonggeun Son) in Soonchunhyang (SCH) University

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the 3S-Smart Software Solutions support team [5].

8 Disclaimer

3S-Smart Software Solutions GmbH assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided on good faith by 3S-Smart Software Solutions GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of 3S-Smart Software Solutions GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

Bibliography

[1] 3S-Smart Software Solutions GmbH: CODESYS Security Whitepaper
[2] 3S-Smart Software Solutions GmbH: Coordinated Disclosure Policy
[3] 3S-Smart Software Solutions GmbH CODESYS update area: https://www.codesys.com/download
[4] 3S-Smart Software Solutions GmbH security information page: https://www.codesys.com/security
[5] 3S-Smart Software Solutions GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[8] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-08_CDS-62813.pdf

Change History

Version	Description	Date
1.0	First version	22.07.2019
2.0	Public reference added, release date of fix version updated	18.12.2019